

Report Tecnico: Windows Server 2022 Configuration

Scenario: Infrastruttura IT
"Stark Industries / Avengers Tower"

Autore: Josh Van Edward Abanico
Corso: Cyber Security & Ethical Hacking
Data: 13 febbraio 2026



Obiettivo: Configurazione Domain Controller, Active Directory e
Gestione Accessi

Sistema Operativo: Windows Server 2022

Indice

1 Introduzione e Scenario	2
1.1 Obiettivi del Progetto	2
2 Fase 1: Configurazione Iniziale del Server	2
2.1 Identificazione e Rinomina del Sistema	2
3 Fase 2: Promozione a Domain Controller	3
3.1 Creazione della Foresta	3
3.2 Verifica dell'Installazione	3
4 Fase 3: Gestione Active Directory	4
4.1 Struttura delle Organizational Units (OU)	4
4.2 Creazione Utenti	4
4.3 Organizzazione in Gruppi di Sicurezza	5
4.3.1 Gruppo Amministrazione (Tech Lead)	5
4.3.2 Gruppo Comando (Avengers Command)	5
4.3.3 Gruppo Operativo (Heavy Hitters)	6
4.3.4 Gruppo Reclute (Young Avengers)	6
5 Fase 4: Gestione File System e Permessi	7
5.1 Creazione Struttura Cartelle	7
5.2 Configurazione Permessi di Condivisione (Share Permissions)	7
5.2.1 Progetti Armature MK (Top Secret)	8
5.2.2 Ordini Missione (Operativo)	9
5.2.3 Bacheca Avvisi Tower (Pubblica Lettura)	10
5.2.4 Richieste Danni Collaterali (Pubblica Scrittura)	11
5.2.5 Manuali Addestramento (Training)	12
6 Fase 5: Verifica e Testing (Client Side)	13
6.1 Accesso al Dominio	13
6.2 Enumerazione delle Risorse	13
6.3 Test dei Permessi Restrittivi (Accesso Negato)	14
6.4 Test dei Permessi Consentiti (Accesso Riuscito)	15
7 Conclusioni	15

1 Introduzione e Scenario

1.1 Obiettivi del Progetto

L'obiettivo di questa attività è la progettazione e l'implementazione di un'infrastruttura di rete basata su Windows Server 2022. Lo scenario simulato riguarda la gestione IT della **Stark Industries** e del team **Avengers**. L'attività comprende la configurazione del server, la promozione a Domain Controller, la strutturazione di Active Directory (Organizational Units, Users, Groups), la gestione dei Permessi di Condivisione (Share Permissions) e la verifica finale lato client.

2 Fase 1: Configurazione Iniziale del Server

2.1 Identificazione e Rinomina del Sistema

In fase di post-installazione, il sistema presentava un hostname generico autogenerato da Windows (WIN-LGIA3O6HCOK), non conforme agli standard aziendali.

Si è proceduto alla modifica del nome computer in **StarkIndustriesServer** per facilitarne l'identificazione in rete e la gestione remota, mantenendo inizialmente il gruppo di lavoro WORKGROUP.

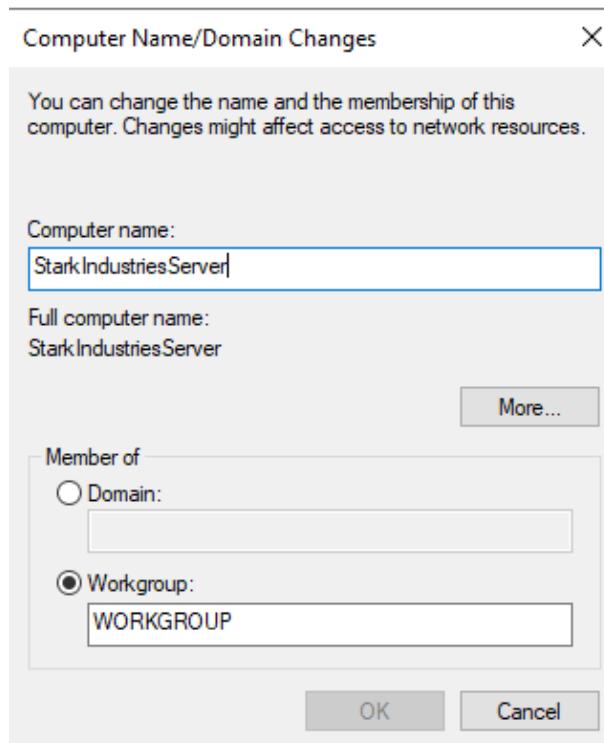


Figura 1: Rinomina del server in StarkIndustriesServer.

3 Fase 2: Promozione a Domain Controller

3.1 Creazione della Foresta

Dopo aver installato il ruolo *Active Directory Domain Services* (AD DS), si è proceduto alla promozione del server a Domain Controller. È stata creata una nuova foresta con Root Domain Name **stark.local**.

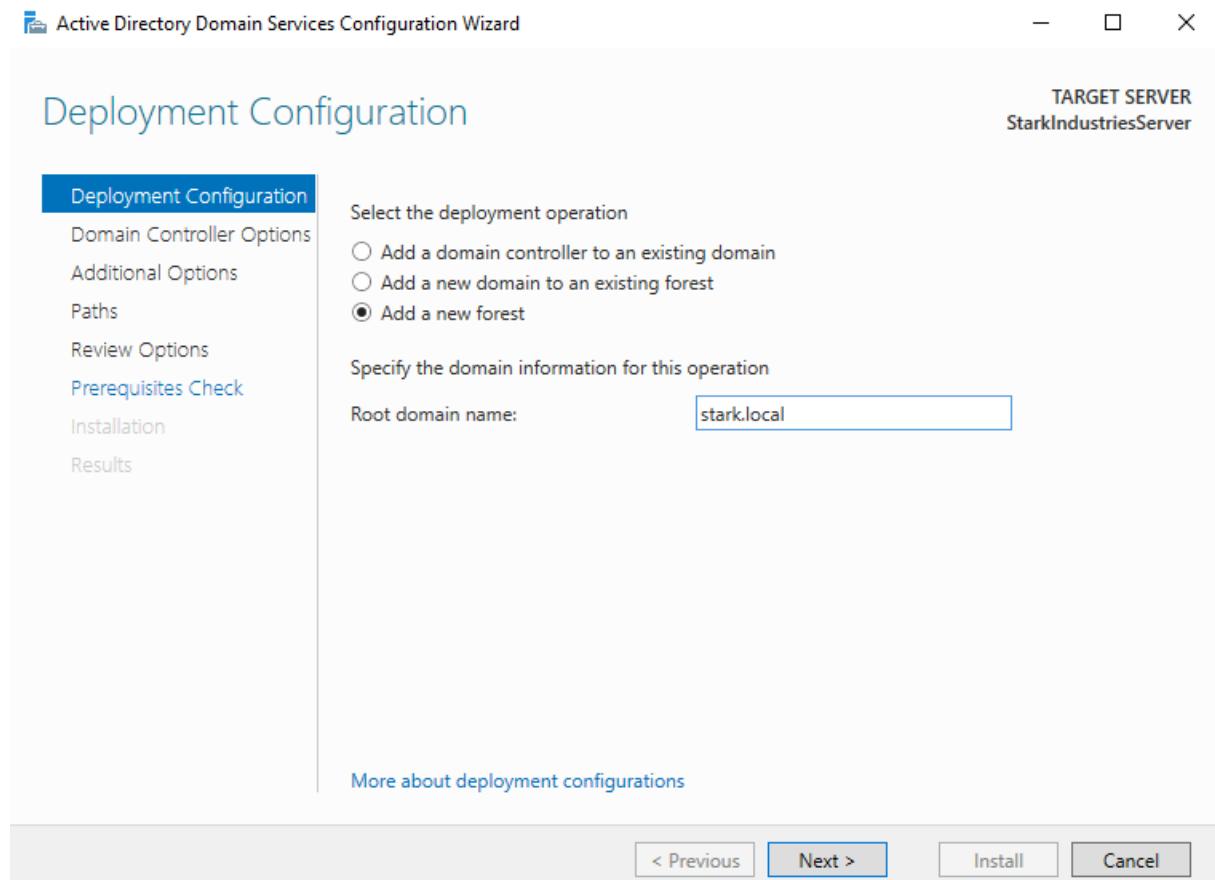


Figura 2: Configurazione del deployment: Nuova foresta stark.local.

3.2 Verifica dell'Installazione

Al termine del processo e dopo il riavvio, il server permette il login come Amministratore di Dominio (STARK\Administrator), confermando il corretto funzionamento del servizio di directory.

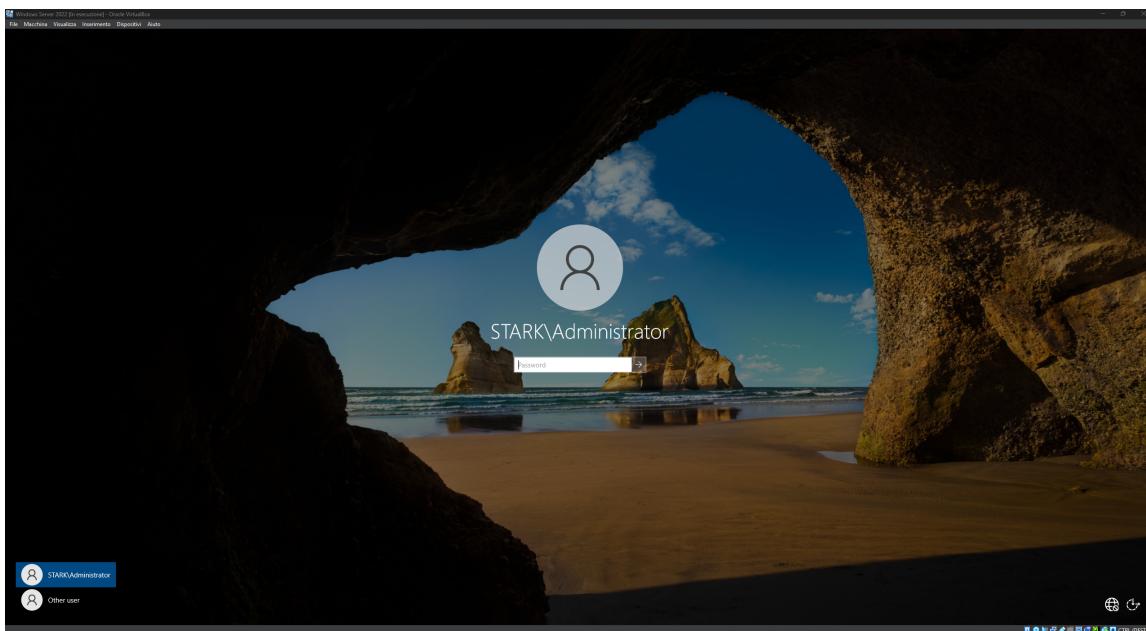


Figura 3: Login screen che conferma l'appartenenza al dominio STARK.

4 Fase 3: Gestione Active Directory

4.1 Struttura delle Organizational Units (OU)

Per garantire una gestione ordinata, è stata creata una struttura gerarchica. È stata definita una OU principale **Stark_Industries** per contenere gli oggetti amministrativi.

4.2 Creazione Utenti

Sono stati creati gli account utente per i membri del team, assegnando username conformi alle policy (es. *TheHulk* per Bruce Banner).

A screenshot of the 'New Object - User' dialog box. The 'Create in:' dropdown is set to 'stark.local/Stark_Industries'. The 'First name' field contains 'Bruce', 'Last name' contains 'Banner', and 'Full name' contains 'Bruce Banner'. In the 'User logon name:' field, 'TheHulk' is entered, followed by '@stark.local'. Below it, 'User logon name (pre-Windows 2000):' shows 'STARK\' and 'TheHulk'. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

Figura 4: Creazione dell'utente Bruce Banner (Logon name: TheHulk).

4.3 Organizzazione in Gruppi di Sicurezza

Gli utenti sono stati suddivisi in dipartimenti logici per riflettere le diverse competenze e livelli di accesso.

4.3.1 Gruppo Amministrazione (Tech Lead)

Include i membri con competenze tecniche elevate (Tony Stark, Bruce Banner) che necessitano di privilegi amministrativi.

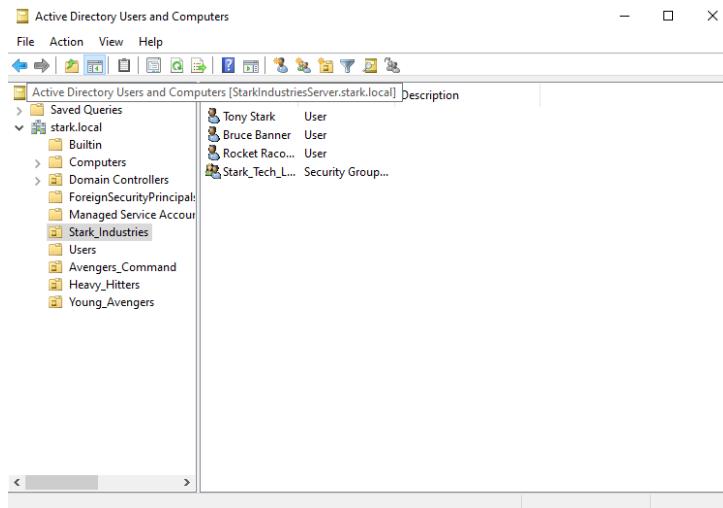


Figura 5: OU Stark_Industries con gli utenti amministrativi.

4.3.2 Gruppo Comando (Avengers Command)

Include i leader tattici (Steve Rogers, Nick Fury, Natasha Romanoff).

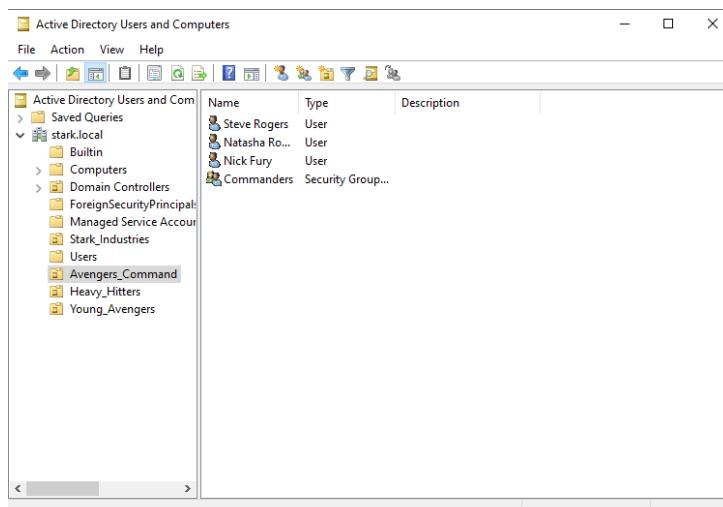


Figura 6: OU Avengers_Command e relativi membri.

4.3.3 Gruppo Operativo (Heavy Hitters)

Include i membri "muscolari" operativi sul campo (Thor, Clint Barton, Drax). A questi utenti è stato assegnato il gruppo **Muscles**.

The screenshot shows the Windows Server Active Directory Users and Computers interface. On the left, the navigation pane displays the tree structure: Active Directory Users and Computers, Saved Queries, stark.local (selected), Builtin, Computers, Domain Controllers, ForeignSecurityPrincipal, Managed Service Account, Stark_Industries, Users, Avengers_Command, Heavy_Hitters (selected), and Young_Avengers. On the right, a table lists objects in the selected 'Heavy_Hitters' container. The table has columns for Name, Type, and Description. It contains four entries: Thor_Odinson (User), Clint_Barton (User), Drax (User), and Muscles (Security Group...).

Name	Type	Description
Thor_Odinson	User	
Clint_Barton	User	
Drax	User	
Muscles	Security Group...	

Figura 7: OU Heavy_Hitters con il gruppo Muscles.

4.3.4 Gruppo Reclute (Young Avengers)

Include i membri junior (Peter Parker, Kate Bishop, Kamala Khan) nel gruppo **rookies**, con permessi limitati.

The screenshot shows the Windows Server Active Directory Users and Computers interface. On the left, the navigation pane displays the tree structure: Active Directory Users and Computers, Saved Queries, stark.local (selected), Builtin, Computers, Domain Controllers, ForeignSecurityPrincipal, Managed Service Account, Stark_Industries, Users, Avengers_Command, Heavy_Hitters, and Young_Avengers (selected). On the right, a table lists objects in the selected 'Young_Avengers' container. The table has columns for Name, Type, and Description. It contains four entries: Peter_Parker (User), Kate_Bishop (User), Kamala_Khan (User), and rookies (Security Group...).

Name	Type	Description
Peter_Parker	User	
Kate_Bishop	User	
Kamala_Khan	User	
rookies	Security Group...	

Figura 8: OU Young_Avengers con il gruppo rookies.

5 Fase 4: Gestione File System e Permessi

5.1 Creazione Struttura Cartelle

È stata creata una struttura di directory nel disco locale C: per gestire le risorse condivise.

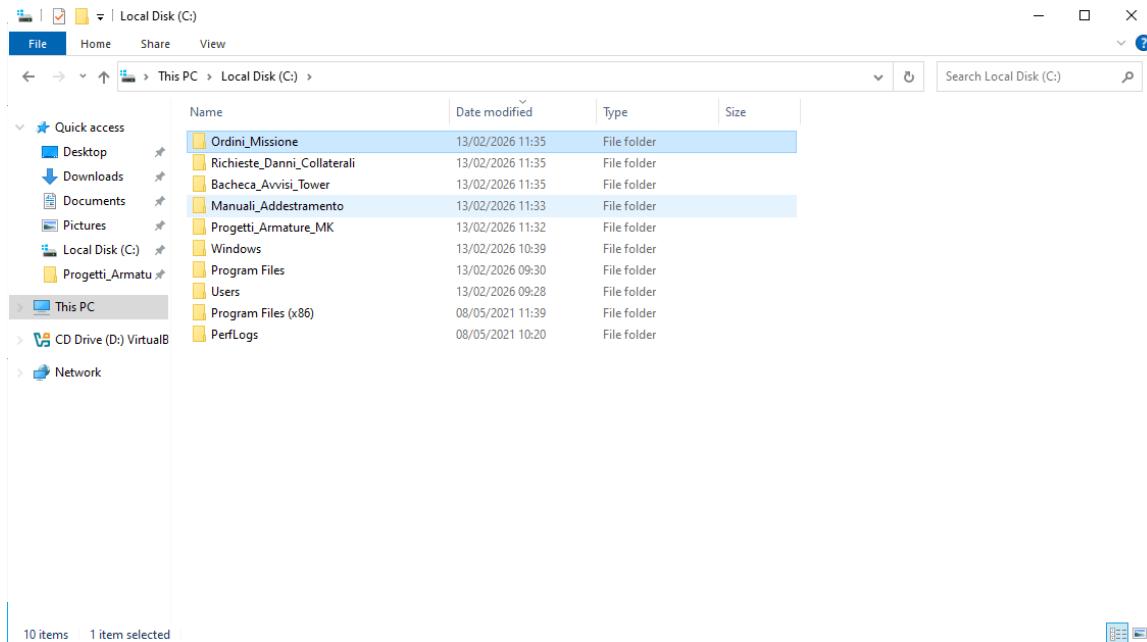


Figura 9: Struttura finale del File System.

5.2 Configurazione Permessi di Condivisione (Share Permissions)

Per la gestione dell'accesso alle risorse tramite rete, sono stati applicati i **Share Permissions** (Permessi di Condivisione) specifici per ogni cartella, seguendo il principio del *Least Privilege*.

Sono stati definiti i seguenti livelli di accesso:

5.2.1 Progetti Armature MK (Top Secret)

Accesso consentito esclusivamente al gruppo **Stark_Tech_Lead** con controllo completo. Gli altri gruppi non hanno accesso.

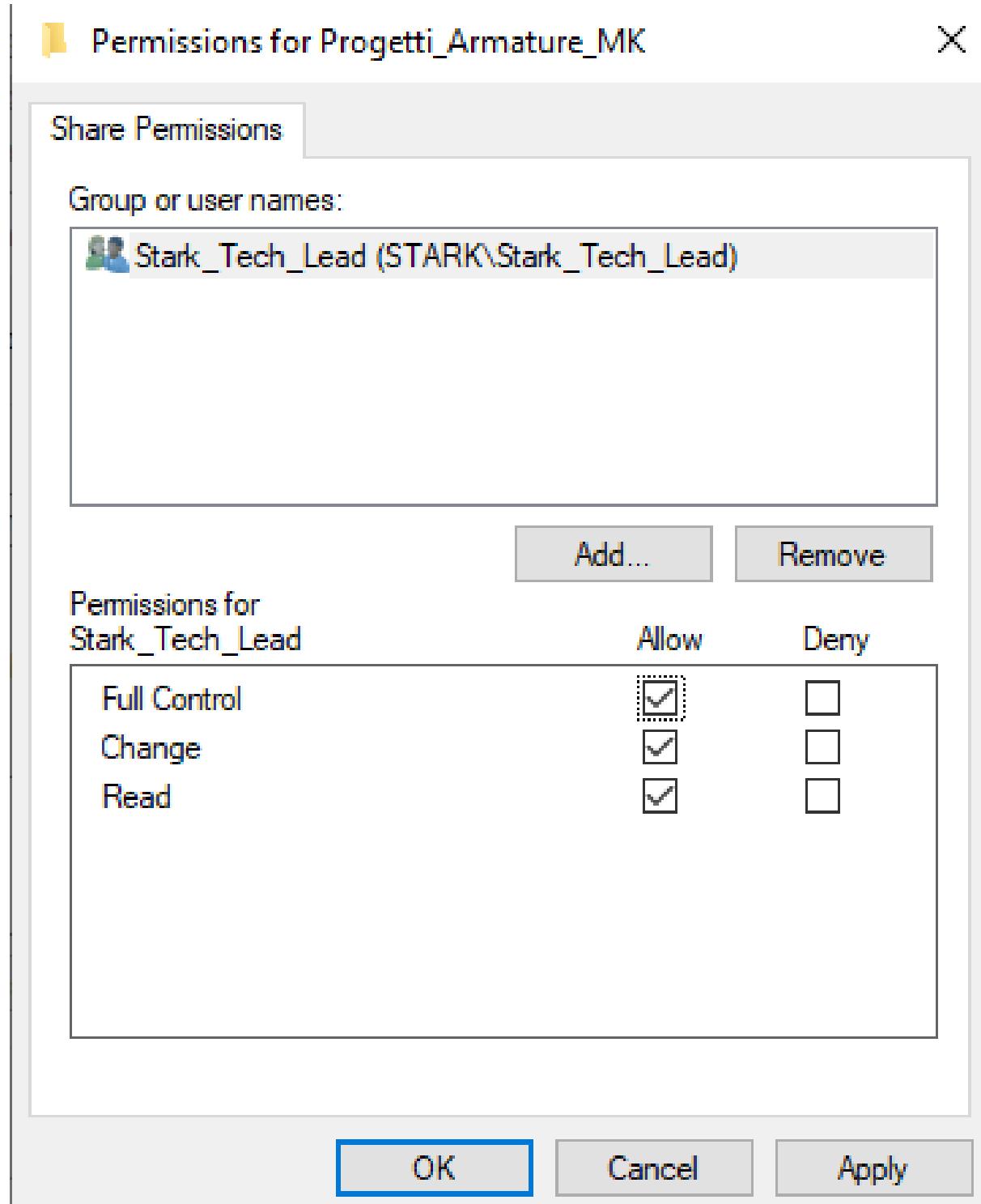


Figura 10: Permessi restrittivi per Progetti_Armature_MK.

5.2.2 Ordini Missione (Operativo)

Il gruppo **Muscles** (Operativi) ha permessi di lettura e modifica (Change/Read), per poter consultare gli ordini ma non alterarli strutturalmente.

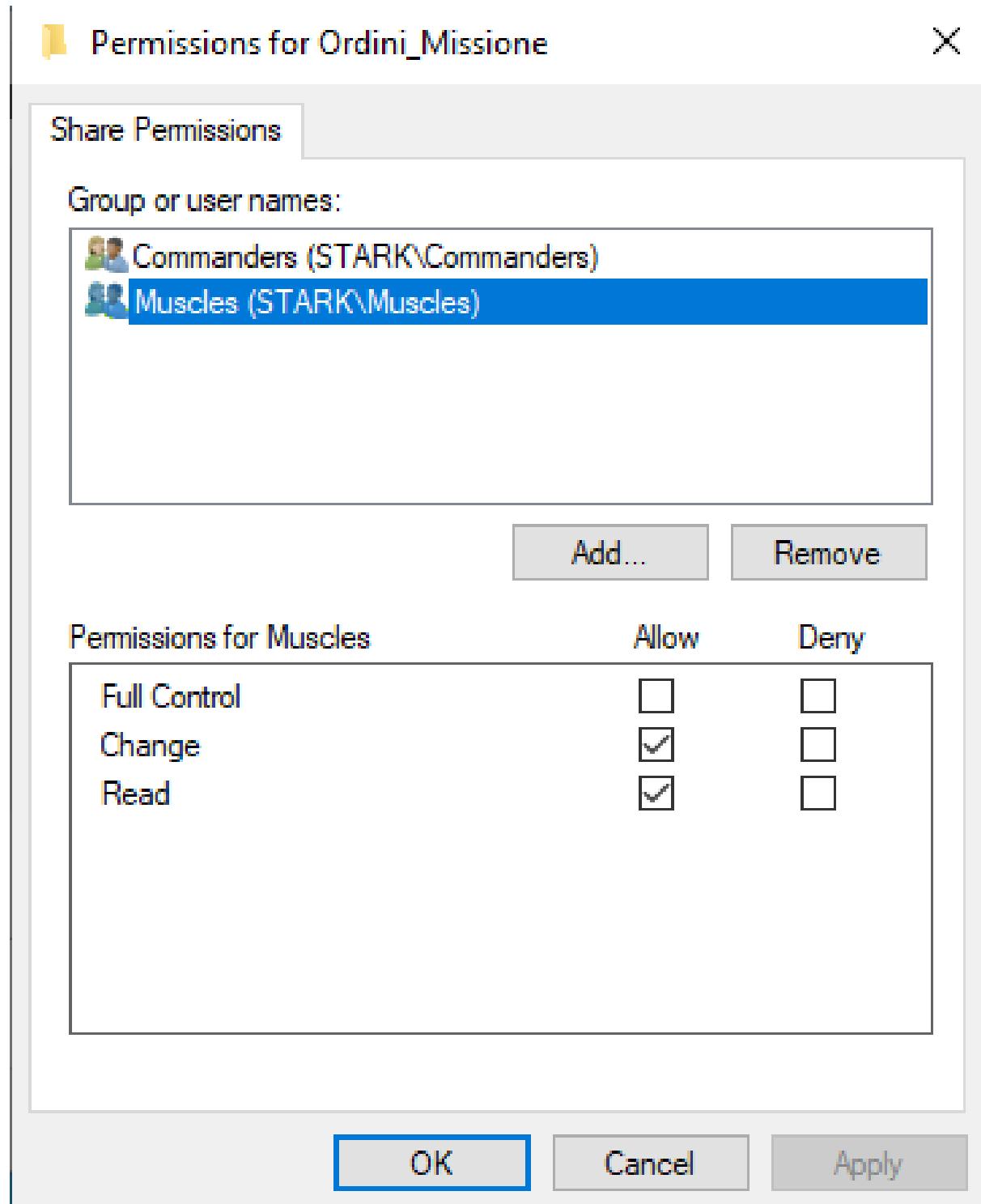


Figura 11: Permessi per Ordini_Missione assegnati al gruppo Muscles.

5.2.3 Bacheca Avvisi Tower (Pubblica Lettura)

Tutti gli utenti del dominio (**Domain Users**) possono leggere gli avvisi, ma non modificarli. Solo gli amministratori hanno il controllo completo.

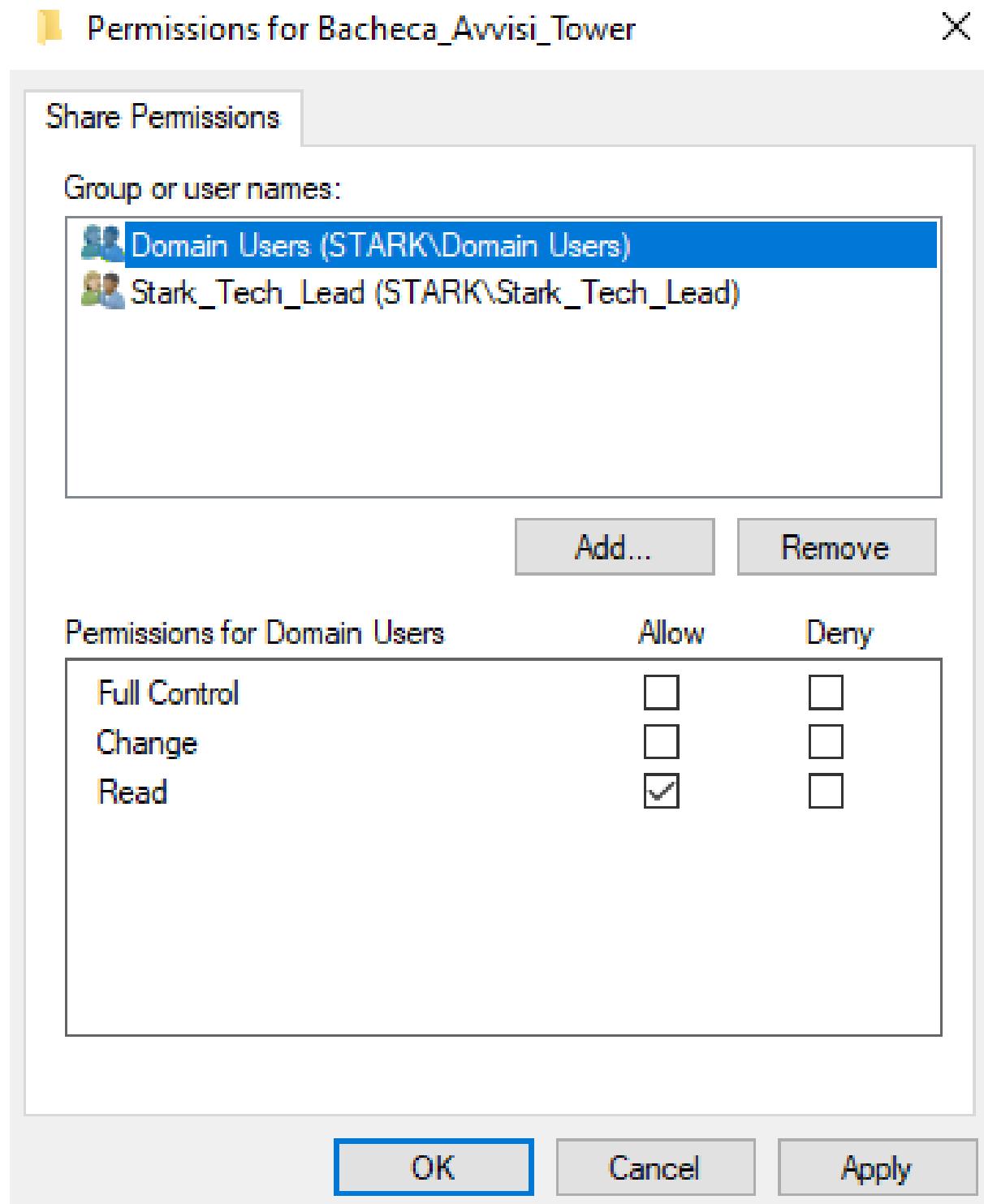


Figura 12: Permessi di sola lettura per Domain Users sulla Bacheca.

5.2.4 Richieste Danni Collaterali (Pubblica Scrittura)

Cartella destinata all'upload di report. Agli utenti del dominio (**Domain Users**) è stato concesso il permesso di modifica (Change) per poter caricare file.

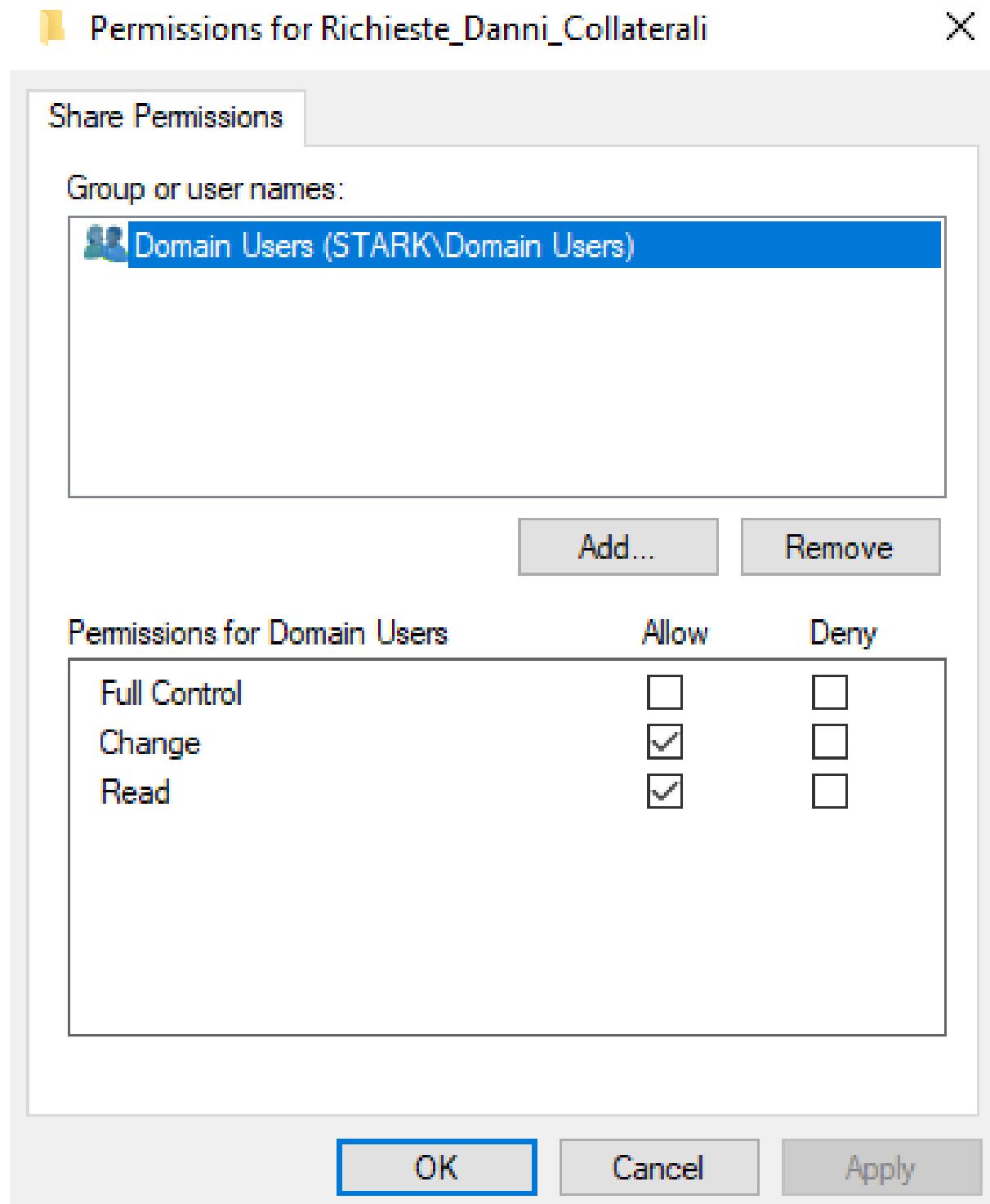


Figura 13: Permessi di scrittura per Domain Users su Richieste_Danni_Collaterali.

5.2.5 Manuali Addestramento (Training)

Il gruppo **rookies** (Reclute) ha accesso in sola lettura (Read). Non possono modificare i manuali.

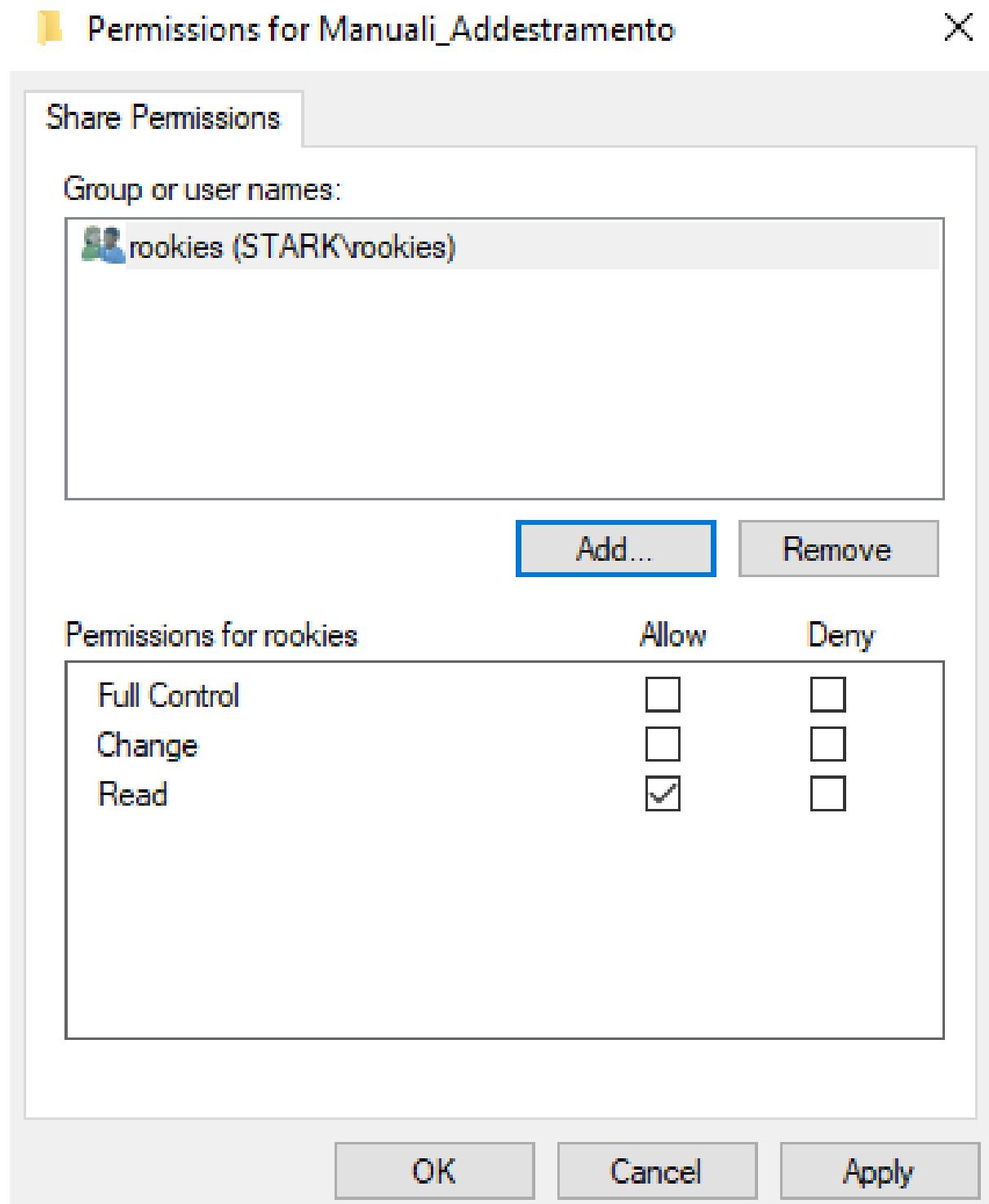


Figura 14: Permessi di lettura per il gruppo rookies sui Manuali.

6 Fase 5: Verifica e Testing (Client Side)

Per validare la configurazione dei permessi e delle condivisioni, è stato utilizzato un client Windows 10 connesso al dominio *stark.local*.

6.1 Accesso al Dominio

È stato effettuato il login utilizzando le credenziali dell'utente **Spiderman** (Peter Parker), appartenente al gruppo *rookies* (Young Avengers).

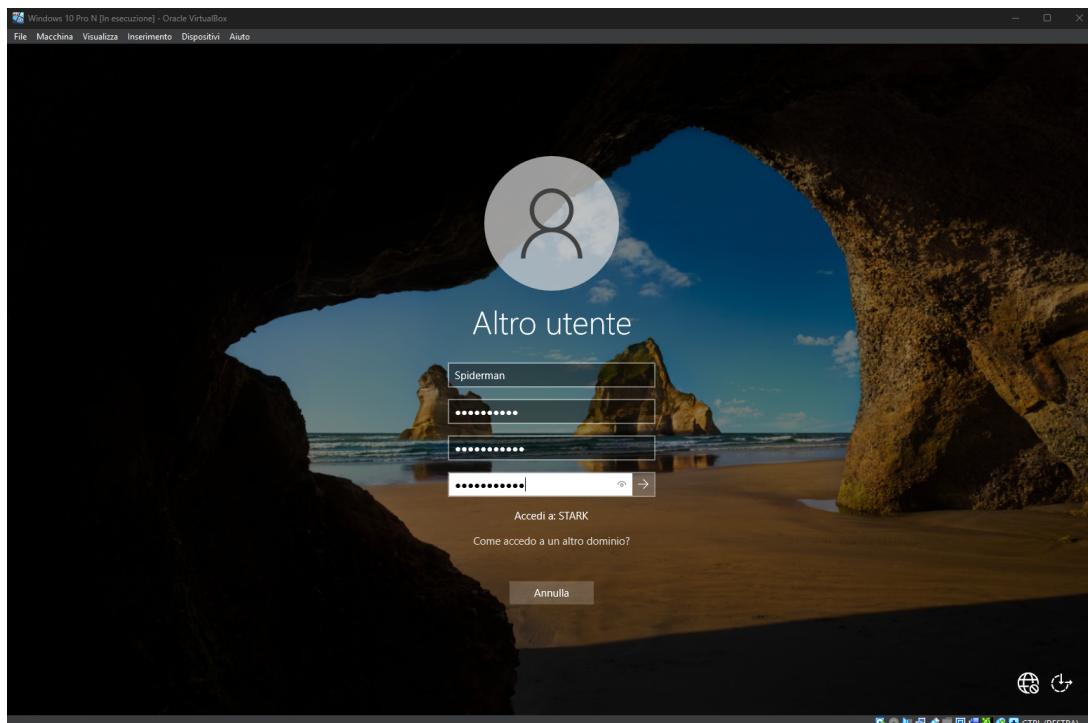


Figura 15: Login al client con utente Spiderman.

6.2 Enumerazione delle Risorse

Accedendo al percorso di rete del server (\\\StarkIndustriesServer), l'utente è in grado di visualizzare le cartelle condivise.

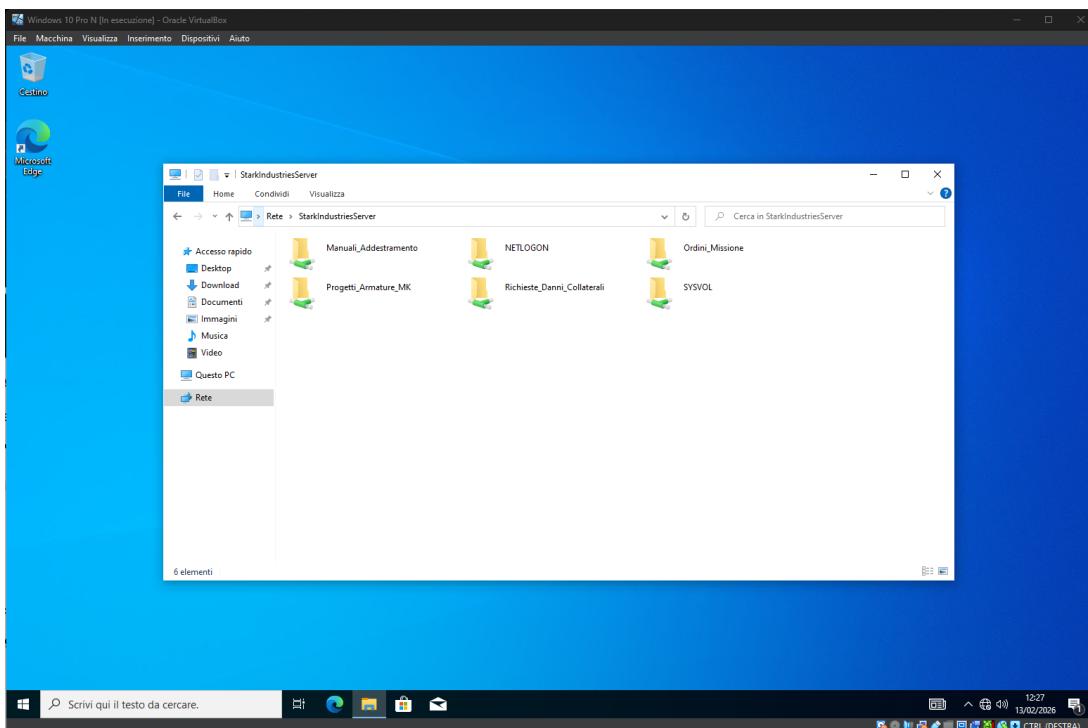


Figura 16: Visualizzazione delle share di rete.

6.3 Test dei Permessi Restrittivi (Accesso Negato)

Tentando di accedere alla cartella **Progetti_Armature_MK**, riservata agli amministratori, il sistema nega correttamente l'accesso. Questo conferma che la policy di sicurezza per il gruppo *rookies* è attiva e funzionante.

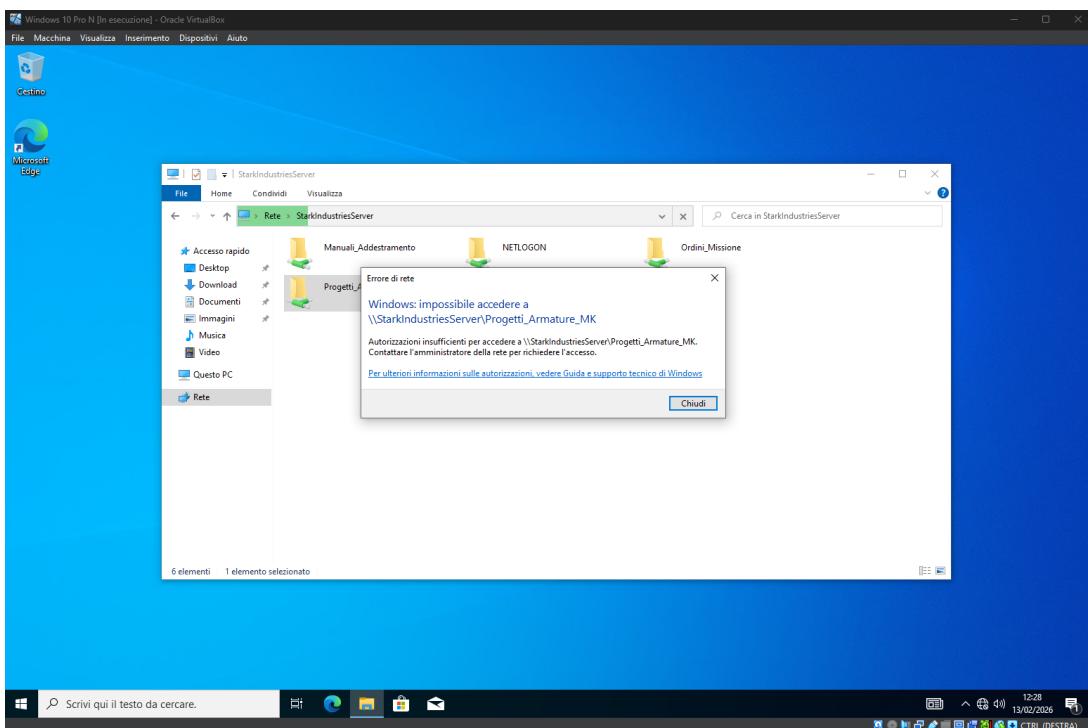


Figura 17: Verifica Accesso Negato sulla cartella riservata.

6.4 Test dei Permessi Consentiti (Accesso Riuscito)

Tentando invece di accedere alla cartella **Manuali_Addestramento**, per la quale il gruppo ha permessi di lettura, l'operazione ha successo e i file sono visibili.

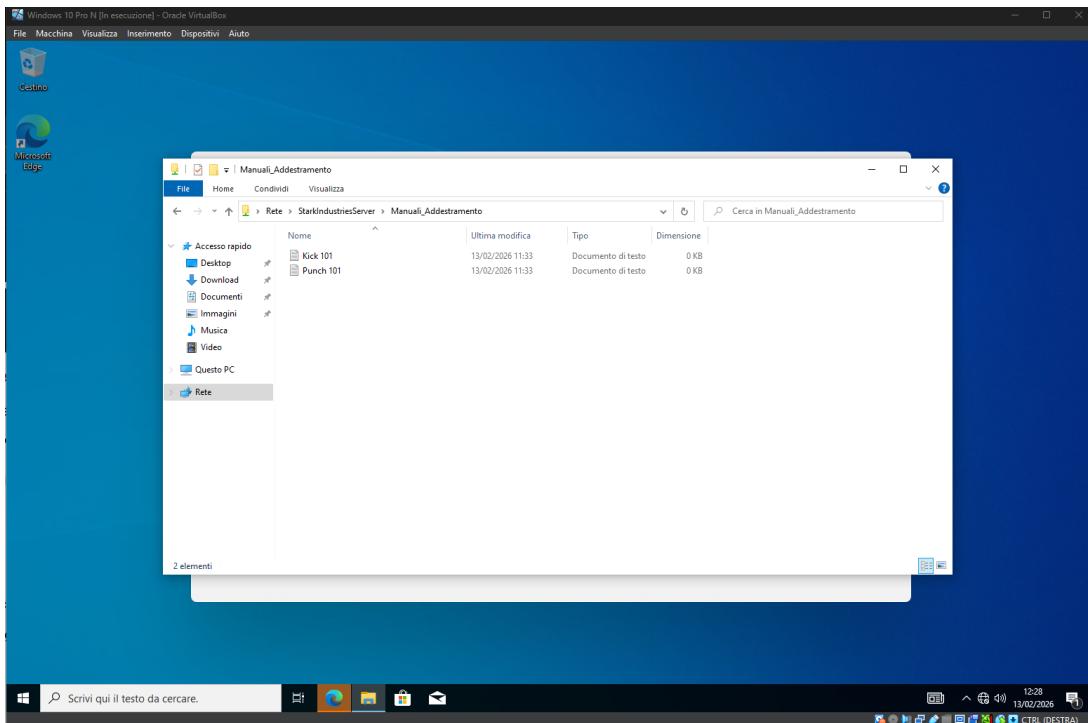


Figura 18: Accesso riuscito alla cartella Manuali.

7 Conclusioni

L'esercitazione ha permesso di configurare con successo un Domain Controller Windows Server 2022. La struttura creata rispecchia una gerarchia aziendale complessa (Stark Industries), dimostrando la capacità di gestire:

- Identità e Accessi tramite Active Directory.
- Organizzazione logica tramite OU e Gruppi.
- Sicurezza dei dati tramite Permessi di Condivisione (Share Permissions).
- Verifica funzionale tramite client in dominio.